

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-223228

(43)Date of publication of application : 09.08.2002

(51)Int.Cl. H04L 12/46  
G06F 15/00  
H04L 12/44  
H04L 12/66

(21)Application number : 2001-347008 (71)Applicant : ALCATEL  
INTERNETWORKING INC  
(22)Date of filing : 13.11.2001 (72)Inventor : HAYS JEFF  
MARTIN CHRISTOPHER

(30)Priority

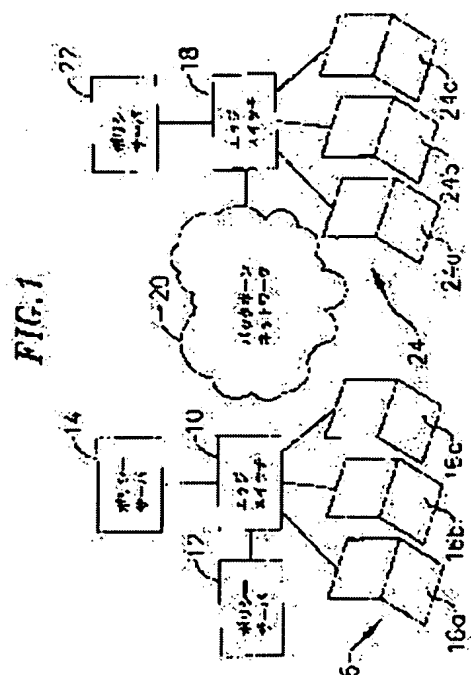
Priority number : 2000 715281 Priority date : 17.11.2000 Priority country : US

## (54) INTEGRATED POLICY IMPLEMENTATION SERVICE FOR COMMUNICATION NETWORK

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an integrated policy implementation service for a communication network where user authentication is integrated with QoS provision.

**SOLUTION:** This integrated policy implementation service includes a data communication switch connected to one or more policy servers. The switch transmits requests for user and device information to end devices connected to a network. The devices respond by transmitting responses including the user and device information to the switch. The switch transmits the user and device information to the one or more policy servers for user authentication and QoS provision. The one or more policy servers respond by transmitting authentication information and QoS information to the switch. The switch uses the authentication information to determine whether to enable a network interface used by the user to communicate with the network.



---

**LEGAL STATUS**

[Date of request for examination] 09.11.2004

[Date of sending the examiner's decision of rejection] 24.10.2006

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2002-223228

(P2002-223228A)

(43)公開日 平成14年8月9日(2002.8.9)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード*(参考)
H 0 4 L 12/46		H 0 4 L 12/46	A 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 K 0 3 0
H 0 4 L 12/44	3 0 0	H 0 4 L 12/44	3 0 0 5 K 0 3 3
12/66		12/66	A

審査請求 未請求 請求項の数35 O L 外国語出願 (全 47 頁)

(21)出願番号 特願2001-347008(P2001-347008)  
(22)出願日 平成13年11月13日(2001.11.13)  
(31)優先権主張番号 7 1 5 2 8 1  
(32)優先日 平成12年11月17日(2000.11.17)  
(33)優先権主張国 米国 (U S)

(71)出願人 500086283  
アルカテル・インターネットワーキング・  
インコーポレイテッド  
アメリカ合衆国、カリフォルニア・91301、  
カラバサス、ウエスト・アグーラ・ロー  
ド・26801  
(72)発明者 ジェフ・ヘイズ  
アメリカ合衆国、ユタ・84003、ハイラン  
ド、ウエスト・10570・ノース・6389  
(74)代理人 100062007  
弁理士 川口 義雄 (外5名)

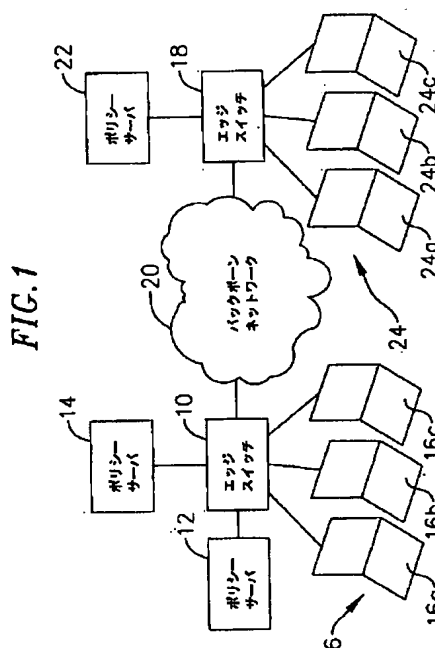
最終頁に続く

(54)【発明の名称】 通信ネットワークのための統合ポリシー実施サービス

(57)【要約】

【課題】 ユーザ認証がQoS提供と統合された通信ネットワークのための統合ポリシー実施サービスを提供すること。

【解決手段】 このサービスは、1つまたは複数のポリシーサーバに接続されたデータ通信スイッチを含む。スイッチは、ネットワークに接続された終端デバイスに、ユーザ情報およびデバイス情報を求める要求を送信する。そのデバイスは、ユーザ情報およびデバイス情報を含んだ応答をスイッチに送信することによって応答する。スイッチは、ユーザ認証およびQoS提供のために、そのユーザ情報およびデバイス情報を1つまたは複数のポリシーサーバに送信する。この1つまたは複数のポリシーサーバは、認証情報およびQoS情報をスイッチに送信することによって応答する。スイッチは、その認証情報を使用して、ネットワークと通信するのにユーザによって使用されるネットワークインターフェースを使用可能にするかどうかを判定する。



【特許請求の範囲】

【請求項1】 通信ネットワークのための統合ポリシー実施サービスで使用するための、端末デバイスおよび1つまたは複数のポリシーサーバを含む通信ネットワーク内のデータ通信スイッチであって、  
端末デバイスに複数の情報を求める要求を送信するための手段と、  
端末デバイスから要求した複数の情報を受信するための手段と、

1つまたは複数のポリシーサーバに、受信した複数の情報を同時に送信するための手段と、

1つまたは複数のポリシーサーバから、送信された複数の情報に基づくユーザ認証情報およびサービス品質情報を同時に受信するための手段とを含むデータ通信スイッチ。

【請求項2】 複数の情報が、ユーザ情報およびデバイス情報を含む請求項1に記載のデータ通信スイッチ。

【請求項3】 スイッチが、1つのポリシーサーバと通信し、1つのポリシーサーバが、  
ユーザ認証情報を検索するための手段と、  
サービス品質情報を検索するための手段とを含む請求項1に記載のデータ通信スイッチ。

【請求項4】 スイッチが、2つのポリシーサーバと通信し、第1のポリシーサーバが、ユーザ認証情報を検索するための手段を含み、かつ第2のポリシーサーバが、サービス品質情報を検索するための手段を含む請求項1に記載のデータ通信スイッチ。

【請求項5】 ユーザ認証情報に応答してネットワークリソースを未認証状態から認証済み状態に移させるための手段をさらに含む請求項1に記載のデータ通信スイッチ。

【請求項6】 サービス品質情報に応答して、端末デバイスから受信したデータフローに関してサービス品質をスイッチ上で実施するための手段をさらに含む請求項1に記載のデータ通信スイッチ。

【請求項7】 ユーザ認証情報が、許可されたネットワークリソースのリストを含む請求項1に記載のデータ通信スイッチ。

【請求項8】 サービス品質情報が、端末デバイスから受信したデータフローに適用されるサービス品質処理を含む請求項1に記載のデータ通信スイッチ。

【請求項9】 単一のポリシーサーバをサポートする第1のモードと、  
2つのポリシーサーバをサポートする第2のモードと、  
前記第1のモードと第2のモードの間で選択する手段とをさらに含む請求項1に記載のデータ通信スイッチ。

【請求項10】 通信ネットワークのための統合ポリシー実施サービスで使用するための、端末デバイスおよびポリシーサーバを含む通信ネットワーク内のデータ通信スイッチであって、

端末デバイスに複数の情報を求める要求を送信し、端末デバイスから要求した複数の情報を受信する第1のネットワークインターフェースと、

第1のネットワークインターフェースに結合された管理インターフェースであって、受信した複数の情報をポリシーサーバに送信し、ポリシーサーバが、複数の情報に  
応答してユーザ認証情報およびQoS情報を検索して、  
検索したユーザ認証情報およびQoS情報を管理インターフェースに同時に通信するインターフェースと、  
ユーザ認証情報に  
応答して、ネットワークリソースを未認証状態から認証済み状態に移させる、管理インターフェースに結合された第1のドライバと、  
サービス品質情報に  
応答して、端末デバイスから受信したデータフローに関してサービス品質をスイッチ上で実施する、管理インターフェースに結合された第2のドライバとを含むデータ通信スイッチ。

【請求項11】 複数の情報が、ユーザ情報およびデバイス情報を含む請求項10に記載のデータ通信スイッチ。

【請求項12】 ユーザ認証情報が、許可されたネットワークリソースのリストを含む請求項10に記載のデータ通信スイッチ。

【請求項13】 サービス品質情報が、端末デバイスから受信したデータフローに適用されるサービス品質処理を含む請求項10に記載のデータ通信スイッチ。

【請求項14】 通信ネットワークのための統合ポリシー実施サービスで使用するための、端末デバイスおよびポリシーサーバを含む通信ネットワーク内のデータ通信スイッチであって、

端末デバイスに複数の情報を求める要求を送信し、端末デバイスから要求した複数の情報を受信する第1のネットワークインターフェースと、

受信した複数の情報をポリシーサーバに単一の制御フローで送信し、ユーザ認証情報およびサービス品質情報をポリシーサーバから該制御フローで受信する、第1のネットワークインターフェースに結合された管理インターフェースと、

ユーザ認証情報に  
応答して、ネットワークリソースを未認証状態から認証済み状態に移させる、管理インターフェースに結合された第1のドライバと、  
サービス品質情報に  
応答して、端末デバイスから受信したデータフローに関してサービス品質をスイッチ上で実施する、管理インターフェースに結合された第2のドライバとを含むデータ通信スイッチ。

【請求項15】 複数の情報が、ユーザ情報およびデバイス情報を含む請求項14に記載のデータ通信スイッチ。

【請求項16】 ユーザ認証情報が、許可されたネットワークリソースのリストを含む請求項14に記載のデータ通信スイッチ。

【請求項 17】 サービス品質情報が、端末デバイスから受信したデータフローに適用されるサービス品質処理を含む請求項 14 に記載のデータ通信スイッチ。

【請求項 18】 通信ネットワークのための統合ポリシー実施サービスで使用するための、端末デバイス、第 1 のポリシーサーバおよび第 2 のポリシーサーバを含む通信ネットワーク内のデータ通信スイッチであって、端末デバイスに複数の情報を求める要求を送信し、端末デバイスから要求した複数の情報を受信する第 1 のネットワークインターフェースと、第 1 のポリシーサーバに第 1 の制御フローで複数の情報の第 1 の部分を送信して、第 1 のポリシーサーバから該第 1 の制御フローでユーザ認証情報を受信し、さらに、第 2 のポリシーサーバに第 2 の制御フローで複数の情報の第 2 の部分を送信して、第 2 のポリシーサーバから第 2 の制御フローでサービス品質情報を受信する、第 1 のネットワークインターフェースに結合された管理インターフェースであって、第 1 の制御フローが、第 2 の制御フローと同時に行われるインターフェースと、ユーザ認証情報にตอบสนองして、ネットワークリソースを未認証状態から認証済み状態に移させる、管理インターフェースに結合された第 1 のドライバと、サービス品質情報にตอบสนองして、端末デバイスから受信したデータフローに関してサービス品質をスイッチ上で実施する、管理インターフェースに結合された第 2 のドライバとを含むデータ通信スイッチ。

【請求項 19】 複数の情報が、ユーザ情報およびデバイス情報を含む請求項 18 に記載のデータ通信スイッチ。

【請求項 20】 ユーザ認証情報が、許可されたネットワークリソースのリストを含む請求項 18 に記載のデータ通信スイッチ。

【請求項 21】 サービス品質情報が、スイッチ上で受信したデータフローに適用されるサービス品質処理を含む請求項 18 に記載のデータ通信スイッチ。

【請求項 22】 端末デバイスおよび 1 つまたは複数のポリシーサーバを含む通信ネットワーク内で、該ネットワークのための統合ポリシー実施サービスのための方法であって、端末デバイスに複数の情報を求める要求を送信するステップと、

1 つまたは複数のポリシーサーバに受信した複数の情報を送信するステップと、

1 つまたは複数のポリシーサーバから、送信した複数の情報に基づくユーザ認証情報およびサービス品質情報を同時に受信するステップとを含む、ネットワークのための統合ポリシー実施サービスのための方法。

【請求項 23】 複数の情報が、ユーザ情報およびデバ

イス情報を含む請求項 22 に記載の方法。

【請求項 24】 ユーザ認証情報を検索するステップと、サービス品質情報を検索するステップとをさらに含む請求項 22 に記載の方法。

【請求項 25】 ユーザ認証情報にตอบสนองして、ネットワークリソースを未認証状態から認証済み状態に移させるステップをさらに含む請求項 22 に記載の方法。

【請求項 26】 サービス品質情報にตอบสนองして、端末デバイスから受信したデータフローに関してサービス品質をスイッチ上で実施するステップをさらに含む請求項 22 に記載の方法。

【請求項 27】 ユーザ認証情報が、許可されたネットワークリソースのリストを含む請求項 22 に記載の方法。

【請求項 28】 サービス品質情報が、スイッチ上で受信したデータフローに適用されるサービス品質処理を含む請求項 22 に記載の方法。

【請求項 29】 単一のポリシーサーバをサポートする第 1 のモードと 2 つのポリシーサーバをサポートする第 2 のモードの間で選択するステップをさらに含む請求項 22 に記載の方法。

【請求項 30】 端末デバイス、第 1 のポリシーサーバおよび第 2 のポリシーサーバと通信するスイッチを含む通信ネットワーク内で、該ネットワークのための統合ポリシー実施サービスのための方法であって、端末デバイスに複数の情報を求める要求を送信するステップと、端末デバイスから要求した複数の情報を受信するステップと、第 1 のポリシーサーバに第 1 の制御フローで複数の情報の第 1 の部分を送信して、第 1 のポリシーサーバから第 1 の制御フローでユーザ認証情報を受信するステップと、第 2 のポリシーサーバに第 2 の制御フローで複数の情報の第 2 の部分を送信して、第 2 のポリシーサーバから第 2 の制御フローでサービス品質情報を受信するステップとを含み、第 1 の制御フローが、第 2 の制御フローと同時に行われる、ネットワークのための統合ポリシー実施サービスのための方法。

【請求項 31】 複数の情報が、ユーザ情報およびデバイス情報を含む請求項 30 に記載の方法。

【請求項 32】 ユーザ認証情報にตอบสนองして、ネットワークリソースを未認証状態から認証済み状態に移させるステップをさらに含む請求項 30 に記載の方法。

【請求項 33】 サービス品質情報にตอบสนองして、端末デバイスから受信したデータフローに関してサービス品質をスイッチ上で実施するステップをさらに含む請求項 30 に記載の方法。

【請求項34】 ユーザ認証情報が、許可されたネットワークリソースのリストを含む請求項30に記載の方法。

【請求項35】 サービス品質情報が、スイッチ上で受信したデータフローに適用されるサービス品質処理を含む請求項30に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般にデータ通信ネットワークに関し、より詳細には、ユーザ認証およびサービス品質提供（provisioning）を単一ポリシーサービスに統合するデータ通信ネットワークに関する。

【0002】

【従来の技術】 データ通信ネットワークは、ますますインテリジェントになってきている。ネットワークのインテリジェンスを高めている1つのサービスは、ユーザ認証である。ユーザ認証は、あるユーザがネットワーク内で通信することができるかどうかという問題に答える。従来のネットワークは、ネットワークに対する無制限のアクセスをユーザに提供していたが、より新しい従来ネットワークは、ユーザが通信することを、そのユーザの識別を検証してから、はじめて許可し、このとき、ユーザにあるサブセットのネットワークデバイスだけを使用して通信するのを許すことすらできる。

【0003】 ネットワークのインテリジェンスを高める別のサービスは、サービス品質（QoS）提供である。QoS提供は、そのネットワークであるユーザがどれだけ良好に通信することができるかという問題に対処する。従来のネットワークは、先入れ先出しパケット送達（first-in-time packet delivery）を提供していたが、より新しい従来ネットワークは、先入れ先出しパケット配列を離れ、異なるデータフローに対して異なるQoSを提供している。

【0004】 QoSは、ネットワーク上で見られるフローにポリシー規則を提供する。ポリシー規則は、一般に、フロー条件構成要素およびQoS処理構成要素を含み、特定の条件を満たすフローに対してどのような処理が適用されるべきかという問題に答える。例えば、単純なポリシー規則は、「グループ2内のトラフィックを優先順位レベル3で扱え」という形式をとることができ、この場合、フロー条件は「グループ2」であり、またQoS処理は「優先順位レベル3」である。

【0005】 ユーザ認証サービスおよびQoS提供サービスは、よりインテリジェントなネットワークを作るが、これらのサービスは、緊密に統合されていない。通常、QoS提供タスクは、ユーザ認証タスクが成功のうちに完了してから、はじめて開始される。したがって、作業（effort）の重複および不必要な遅延が、そのような逐次化されたポリシー提供からもたらされてい

る。

【0006】

【発明が解決しようとする課題】 本発明は、ユーザ認証がQoS提供と統合された、通信ネットワークのための統合ポリシー実施サービスを備える。

【0007】

【課題を解決するための手段】 本発明の一態様では、データ通信スイッチが、単一の統合ポリシーサーバを介して統合ポリシー実施サービスをサポートする。このスイッチは、終端デバイスにユーザ情報およびデバイス情報を求める要求を送信し、その終端デバイスから、この要求したユーザ情報およびデバイス情報を受信する第1のネットワークインターフェースを含む。ユーザ情報は、ユーザ識別子およびユーザパスワードを含むことができる。デバイス情報は、例えば、MACアドレス、インターネットプロトコル（IP）アドレス、および仮想LAN（VLAN）識別子などのレイヤ2情報および／またはレイヤ3情報を含むことができる。

【0008】 データ通信スイッチは、管理インターフェースとポリシーサーバの間での単一制御フローで、受信したユーザ情報およびデバイス情報をポリシーサーバに送信し、ユーザ認証情報およびサービス品質情報を受信する管理インターフェースを含む。認証情報は、ACK/NACK標識（indicator）および／または許可されたポートまたはデバイスのリストを含むことができる。QoS情報は、優先順位情報および最大帯域幅情報を含むことができる。

【0009】 また、データ通信スイッチは、ユーザ認証情報に回答して、ネットワークリソースを未認証状態から認証済み状態に遷移させる、例えば、ポートドライバなどの第1のドライバも含む。さらに、例えば、QoSドライバなどの第2のドライバが、サービス品質情報に回答して、データ通信スイッチから受信したデータフローに関して、そのスイッチ上でサービス品質を実施する。

【0010】 本発明の別の態様では、データ通信スイッチは、2つの独立ポリシーサーバを介して統合ポリシー実施サービスをサポートする。このスイッチは、受信したユーザ情報を第1の制御フローで第1のポリシーサーバに送信し、この第1のポリシーサーバから第1の制御フローでユーザ認証情報を受信する管理インターフェースを含む。この管理インターフェースは、さらに、受信したデバイス情報を第2の制御フローで第2のポリシーサーバに送信し、この第2のポリシーサーバから第2の制御フローでサービス品質情報を受信する。第1の制御フローおよび第2の制御フローは、好ましくは、並列に行われる。ユーザ認証とQoS提供のそのような並列実行は、従来技術において存在する逐次化されたポリシー提供に関連する遅延を短縮するのを助ける。

【0011】

【発明の実施の形態】図1は、統合ポリシー実施サービスをサポートする通信ネットワークの概略図である。このネットワークは、ポリシーサーバ12、14、およびデバイス16a、16b、16cに結合されたデータ通信スイッチ10を含む。データ通信スイッチ10は、バックボーンネットワーク20を通じて、このバックボーンネットワーク内で動作する1つまたは複数のコアスイッチ（図示せず）を介し、データ通信スイッチ18に結合されている。データ通信スイッチ18もまた、ポリシーサーバ22、およびデバイス24a、24b、24cに結合されている。

【0012】デバイス16、24は、好ましくは、データ通信スイッチ10、18を介する他のデバイスとのパケット化通信のために、それぞれのネットワークインターフェースを有する、例えば、パーソナルコンピュータ、ワークステーション、またはサーバなどのネットワーク終端局である。データ通信スイッチ10、18は、好ましくは、デバイス16、24によって発信されたパケット化通信を転送するために、複数のそれぞれのネットワークインターフェースを有する、例えば、ハブ、ブリッジ、またはルータなどのゲートウェイデバイスである。ポリシーサーバ12、14、22は、好ましくは、データ通信スイッチ10、18に認証サービスおよびQoS提供サービスを提供する。デバイス16、24、データ通信スイッチ10、18、およびポリシーサーバ12、14、22は、ケーブルまたは他の伝送媒体を介して相互接続することができ、またこれらは、例えば、イーサネット（登録商標）、インターネットプロトコル、および非同期転送モード（ATM）などの、様々なデータ通信プロトコルをサポートすることができる。

【0013】統合ポリシー実施サービスは、データ通信スイッチ10およびポリシーサーバ12、14に関連して一般的に議論する。データ通信スイッチ10は、好ましくは、ネットワークに接続されたデバイス16にユーザ情報およびデバイス情報を求める要求を送信する。デバイス16は、好ましくは、スイッチ10にユーザ情報およびデバイス情報を含んだ応答を送信することによって応答する。スイッチ10は、好ましくは、ユーザ認証およびQoS提供のため受信したユーザ情報およびデバイス情報をポリシーサーバ12、14に送信する。ポリシーサーバ12、14は、好ましくは、認証情報およびQoS情報をスイッチ10に送信することによって応答する。スイッチ10は、好ましくは、その認証情報を使用して、ユーザによってそのネットワークと通信するのに使用されるネットワークインターフェースを使用可能にするかどうかを判定する。そのネットワークインターフェースを使用可能にする判定が行われる限り、スイッチは、好ましくは、受信したQoS情報を使用して、そのスイッチ上でQoSを確立する。次に、このQoSが、ユーザによって使用されるデバイスから受信された

トラフィックに適用されて、ネットワークとの通信が行われる。

【0014】本発明の一実施形態によれば、統合ポリシー実施サービス構成は、好ましくは、データ通信スイッチ10およびポリシーサーバ12、14によって例示されるとおり、2つの独立したポリシーサーバを含む。図2は、2つのポリシーサーバ12、14（認証サーバおよびQoSサーバとも呼ぶ）を介して統合ポリシー実施サービスをサポートするデータ通信スイッチ10のより詳細な概略図である。データ通信スイッチ10は、データバス38によってリンクされた、ネットワークインターフェース30、31、32、34、および管理インターフェース36を含む。ネットワークインターフェース30、31、32、34は、様々なインターフェースを介して、デバイス16、バックボーンネットワーク20内のスイッチ、およびポリシーサーバ12、14を相互接続する。

【0015】管理インターフェース36およびネットワークインターフェース30、31、32、34は、データトラフィックを送信および受信するために、データバス38に結合されている。また、管理インターフェース36およびネットワークインターフェース30、31、32、34は、好ましくは、認証情報およびQoS情報を含む管理情報を送信および受信するために、管理バス46にも結合されている。

【0016】管理インターフェース36は、統合ポリシーマネージャ40、ポートドライバ42、およびQoSドライバ44を含む様々なモジュールをサポートする。統合ポリシーマネージャ40、ポートドライバ42、およびQoSドライバ44は、好ましくは、ソフトウェアモジュールである。別法では、このシステムの実装は、ハードウェア、ファームウェア（例えば、アプリケーション専用集積回路または他のカスタマイズした回路）、および/またはソフトウェアの組み合わせで、あるいは当分野で知られている任意の方法で実現することができる。

【0017】本発明の一実施形態によれば、データ通信スイッチ10は、次の方式での統合ポリシー実施をサポートする。統合ポリシーマネージャ40が、管理バス46を介してデバイス16に、ユーザ情報要求およびデバイス情報要求を送信する。

【0018】デバイス16は、データバス38を介してユーザ情報およびデバイス情報を送信することによって応答する。ユーザ情報は、好ましくは、例えば、ユーザIDなどのユーザ識別情報や、例えば、パスワードなどのユーザ署名情報を含む。デバイス情報は、好ましくは、例えば、MACアドレス、IPアドレス、VLAN識別子などの、レイヤ2情報および/またはレイヤ3情報を含む。ただし、そのようなデバイス情報のうちの1つまたは複数の情報（例えば、MACアドレス）が、送

信元学習を介してデータ通信スイッチ10に既に知られている可能性があることを理解されたい。このシナリオでは、知られているデバイスアドレスは、データ通信スイッチに特に送信される必要がない可能性がある。

【0019】ユーザ情報パケットおよびデバイス情報パケットは、管理インターフェース36によってデータベース38から取り込まれ、統合ポリシーマネージャ40に転送される。統合ポリシーマネージャ40は、そのネットワーク内で通信を行うことが、特定のユーザに許可されるかどうかを判定すること、およびそのユーザデバイスに対して指定されるQoSを識別することによりかかる。これに関し、統合ポリシーマネージャ40は、第1の制御フローで、受信したユーザ情報をポリシーサーバのうちの1つ、すなわち、認証サーバ12に送信し、この認証サーバから対応する認証情報を受信する。認証情報は、好ましくは、ACK/NACK標識、許可されたポートのリスト、および/または他の認証処理情報を含む。図2は、単一の認証サーバを示しているが、本発明により動作するネットワークは、1つまたは複数の認証サーバを含むことができる。

【0020】第2の制御フローで、統合ポリシーマネージャ40は、受信したデバイス情報を第2のポリシーサーバ、すなわち、QoSサーバ14に送信し、そのデバイスに関するQoS情報をこのQoSサーバから受信する。QoS情報は、好ましくは、優先順位レベル、最大帯域幅情報等を含む。

【0021】第1の制御フローおよび第2の制御フローは、好ましくは、並列に行われる。ユーザ認証およびQoS提供のそのような並列実行は、逐次化されたポリシー提供に関連する遅延を短縮するのを助ける。

【0022】図3は、認証サーバ12内に記憶されたユーザ認証テーブル50の例としての概略レイアウト図である。認証テーブル50は、例えば、Novell, Inc. から市販されるNetWare（登録商標）などのツールを使用して作成し、編成することができる。1つの例としての実施形態では、認証テーブル50は、様々な仕方で配置することができるが最も有利には各エントリが認証されるべき特定ユーザに固有である順次エントリとして構成される一組のユーザ認証処理情報を適切に含む。テーブル50の特定のエントリは、例えば、識別番号、文字、または番号（number）と文字の組み合わせなどである固有のユーザ識別子52を含むことができる。特定のエントリは、さらに、ネットワークに対するアクセスを求めるユーザを確認するための、例えば、ユーザパスワード54などのユーザ署名を含むことができる。前述のものに加えて、特定のエントリは、特定のユーザに関する時間制限情報56および許可リソース情報58を含むことができる。時間制限情報は、好ましくは、特定のユーザがその間、ネットワークリソースを使用することが許可されている時間、例えば、曜日、

時間帯、および許可されるアクセス持続時間などを定義する。許可されたネットワークリソースのリストは、好ましくは、許可されたネットワークインターフェースおよび/またはデバイスのリストである。

【0023】認証サーバ12は、好ましくは、認証テーブル50を利用し、米国特許第6070243号に記載される方式でユーザを認証する。この特許の内容は、参照により、本明細書に組み込まれる。ユーザ認証のために使用されるプロトコルには、RADIUS、LDAP（Lightweight Directory Access Protocol）、COPS（Common Open Policy Service）、または当分野で知られる他の任意の認証プロトコルが、単独または組み合わせで含まれる。

【0024】ただし、一般に、データ通信スイッチ10からユーザ情報を受信すると、認証サーバ12は、好ましくは、受信した情報をそのサーバ12内に記憶されているユーザ識別情報およびユーザ署名情報と比較する。認証サーバ12は、さらに、そのユーザ識別情報に関連して何らかの時間制限が適用可能かどうかを判定することができる。認証サーバ12は、そのユーザがネットワークリソースの許可されたユーザであること、およびそのログイン試行時にネットワークリソースを使用するのをユーザが許可されていることを確認した場合、好ましくは、ACK指標および/またはユーザが許可されているネットワークリソースのリストをデータ通信スイッチ10に送信する。また、認証サーバ12は、リソースのリストとともに、その使用に適用可能なような時間制限も送信することができる。次に、統合ポリシーマネージャ40は、ポートドライバ42を起動して、ネットワークと通信するためにユーザによって使用されるネットワークインターフェース32上でネットワーク接続性規則を確立する。具体的には、ポートドライバは、好ましくは、許可されたネットワークリソースを未認証状態から認証済み状態に移させることによってそれらのリソースを使用可能にする。また、統合ポリシーマネージャ40は、時間制限情報56に基づいて時間制限処理を実行することもできる。

【0025】図4は、QoSサーバ14内に記憶されたQoSテーブル60の例としての概略レイアウト図である。QoSテーブル60は、好ましくは、一組のフロー条件62、およびそれらのフロー条件のそれぞれに一致するQoS処理64を含む。フロー条件62には、MACアドレス、IPアドレス、VLAN識別子、スロット/ポート識別子、IPプロトコル、インターフェースタイプなどが含まれることが可能である。QoS処理64は、少なくとも優先順位レベルを特定し、このレベルはフロー条件を満たすトラフィックに与えられる優先順位を示す。QoS処理64は、さらに、最大帯域幅、最小帯域幅、ピーク帯域幅、優先順位、待ち時間、ジッタ、



最大待ち行列深度、最大待ち行列バッファなどを示すことができる。

【0026】デバイスから受信したトラフィックに関して適用されるQoSを識別する際、統合ポリシーマネージャ40は、好ましくは、LDAPまたはCOPSを使用して、デバイス情報とともにQoS要求をQoSサーバ14に送信する。デバイス情報を受信すると、QoSサーバ14は、フロー条件を識別して、それに対応するQoS処理をデータ通信スイッチ10に戻す。QoS処理パケットは、管理インターフェース36によってデータベース38から取り入れられて統合ポリシーマネージャ40に転送される。次に、統合ポリシーマネージャ40は、そのQoS処理をスイッチ上で実施するようにQoSドライバ44に通知する。本発明の一実施形態によれば、データ通信スイッチ10は、2000年9月13日出願の「ON-SWITCH POLICY RULE CACHING FOR DATA COMMUNICATION SWITCH」という名称の出願で開示されるように、フロー条件および受信したQoS処理を将来の使用のためにキャッシュ内に記憶することができる。この出願の内容は、参照により、本明細書に組み込まれる。

【0027】図5は、2つのポリシーサーバ12、14を介してスイッチ10によってサポートされる統合ポリシー実施サービスの例としての流れ図である。ステップ70で、管理インターフェース36が、好ましくは、ユーザ情報とデバイス情報の要求をデバイス16に送信する。ステップ72で、管理インターフェース36は、要求したユーザ情報およびデバイス情報をデバイス16から受信する。ステップ74および76によって示される第1の制御フローで、統合ポリシーマネージャ40が、そのユーザ情報とともにユーザ認証要求を認証サーバ12に送信し、そのユーザが認証されたかどうかを示すユーザ認証情報を応答として受信する。

【0028】ステップ78および80によって示される第2の制御フローで、統合ポリシーマネージャ40は、デバイス情報とともにQoS要求をQoSサーバ14に送信し、そのデバイスから発信されたトラフィックに関するQoS情報を応答として受信する。第1の制御フローおよび第2の制御フローは、好ましくは、並列で行われる。

【0029】ステップ82で、ユーザ認証が成功したかどうかに関する照会が行われる。認証が成功であった場合、統合ポリシーマネージャ40が、好ましくは、ポートドライバ42およびQoSドライバ44を起動して、適切なネットワークインターフェースを使用可能にし、また識別されたQoSをデータ通信スイッチ10上で実施する。

【0030】本発明の代替実施形態によれば、統合ポリシー実施サービス構成は、データ通信スイッチ18およ

びポリシーサーバ22によって示されるとおり、単一の統合ポリシーサーバを含む。図6は、この単一ポリシーサーバ22（統合ポリシーサーバとも呼ぶ）を介して統合ポリシー実施サービスをサポートするデータ通信スイッチ18のより詳細な概略図である。データ通信スイッチ18は、データベース100によってリンクされた、ネットワークインターフェース90、92、94、96、および管理インターフェース98を含む。ネットワークインターフェース90、92、94、96は、様々なインターフェースを介して、デバイス24、バックボーンネットワーク20内のスイッチ、統合ポリシーサーバ22を相互接続する。

【0031】管理インターフェース98およびネットワークインターフェース90、92、94、96は、データトラフィックを送信および受信するために、データベース100に結合されている。また、管理インターフェース98およびネットワークインターフェース90、92、94、96は、認証およびQoS情報を含んだ管理情報を送信および受信するために、管理バス102にも結合されている。

【0032】管理インターフェース98は、統合ポリシーマネージャ104、ポートドライバ106、およびQoSドライバ108を含む様々なモジュールをサポートする。ポリシーマネージャ104、ポートドライバ106、およびQoSドライバ108は、好ましくは、ソフトウェアモジュールである。別法では、このシステムの実装は、ハードウェア、ファームウェア（例えば、アプリケーション専用集積回路または他のカスタマイズした回路）、および/またはソフトウェアの組み合わせで、あるいは当分野で知られている任意の方法で実現することができる。

【0033】本発明の一実施形態によれば、データ通信スイッチ18は、下記的方式で統合ポリシー実施をサポートする。統合ポリシーマネージャ104は、好ましくは、管理バス102を介してデバイス24に、ユーザ情報要求およびデバイス情報要求を送信する。

【0034】デバイス24は、データベース100を介してユーザ情報およびデバイス情報を送信することによって応答する。ユーザ情報は、好ましくは、例えば、ユーザIDなどのユーザ識別情報や、例えば、パスワードなどのユーザ署名情報を含む。デバイス情報は、好ましくは、例えば、MACアドレス、IPアドレス、仮想LAN識別子などの、レイヤ2情報および/またはレイヤ3情報を含む。ただし、そのようなデバイス情報のうちの1つまたは複数の情報（例えば、MACアドレス）は、送信元学習を介してデータ通信スイッチ18に既に知られている可能性があることを理解されたい。このシナリオでは、知られているデバイスアドレスは、データ通信スイッチに特に送信される必要がない可能性がある。

【0035】ユーザ情報パケットおよびデバイス情報パ

ケットは、管理インターフェース 98 によってデータベース 100 から取り込まれ、統合ポリシーマネージャ 104 に転送される。統合ポリシーマネージャ 104 は、そのネットワーク内で通信を行うことが、特定のユーザに許可されるかどうかを判定すること、およびそのユーザデバイスに対して指定される QoS を識別することにとりかかる。これに関し、統合ポリシーマネージャ 104 は、好ましくは、単一の制御フローで、受信したユーザ情報およびデバイス情報を統合ポリシーサーバ 22 に送信し、この統合ポリシーサーバ 22 から対応する認証情報および QoS 情報を受信する。認証情報は、好ましくは、ACK/NACK 標識、許可された部分のリスト、および/または他の認証処理情報を含む。QoS 情報は、好ましくは、優先順位レベル、最大帯域幅情報等を含む。

【0036】図 7 は、統合ポリシーサーバ 22 内に記憶されたユーザ認証テーブル 110 の例としての概略レイアウト図である。認証テーブル 110 は、例えば、Novell, Inc. から市販される NetWare (登録商標) などのツールを使用して作成し、編成することができる。1 つの例としての実施形態では、認証テーブル 110 は、様々な仕方で配置することができるが最も有利には各エントリが認証されるべき特定ユーザに固有である順次エントリとして構成された一組のユーザ認証処理情報を適切に含む。テーブル 110 の特定のエントリは、例えば、識別番号、文字、または番号 (number) と文字の組み合わせなどである固有のユーザ識別子 112 を含む。特定のエントリは、さらに、ネットワークに対するアクセスを求めるユーザを確認するための、例えば、ユーザパスワード 114 などのユーザ署名を含むことができる。前述のものに加えて、特定のエントリは、特定のユーザに関する時間制限情報 116 および許可リソース情報 118 を含むことができる。時間制限情報は、好ましくは、特定のユーザがその間、ネットワークリソースを使用することが許可されている、例えば、曜日、時間帯、および許可されるアクセスの持続時間などの時間を定義する。許可されたネットワークリソースのリストは、好ましくは、許可されたネットワークインターフェースおよび/またはデバイスのリストである。

【0037】図 8 は、やはり統合ポリシーサーバ 22 内に記憶された QoS テーブル 120 の例としての概略レイアウト図である。QoS テーブル 120 は、好ましくは、一組のフロー条件 122、およびそれらのフロー条件のそれぞれにマッチする QoS 処理 124 を含む。フロー条件 122 には、好ましくは、MAC アドレス、IP アドレス、VLAN 識別子、スロット/ポート識別子、IP プロトコル、インターフェースタイプなどが含まれる。QoS 処理 124 は、少なくとも優先順位レベルを特定し、このレベルはフロー条件を満たすトラフィ

ックに与えられる優先順位を示す。QoS 処理 124 は、さらに、最大帯域幅、最小帯域幅、ピーク帯域幅、優先順位、待ち時間、ジッタ、最大待ち行列深度、最大待ち行列バッファなどを示すことができる。

【0038】本発明の一実施形態によれば、認証テーブル 110 および QoS テーブル 120 は、統合ポリシーサーバ 22 によってホストされる 1 つまたは複数のデータベース内に記憶される。この 1 つまたは複数のデータベースは、好ましくは、例えば、ハードディスクドライブ、またはドライブアレイなどの 1 つまたは複数の大容量記憶デバイス内に常駐する。

【0039】統合ポリシーサーバ 22 は、好ましくは、認証テーブル 110 を利用し、米国特許第 6070243 号に記載される方式でユーザを認証する。この特許の内容は、参照により、本明細書に組み込まれる。ユーザ認証のために使用されるプロトコルには、RADIUS、LDAP (Lightweight Directory Access Protocol)、COPS (Common Open Policy Service)、または当分野で知られる他の任意の認証プロトコルが、単独または組み合わせで含まれ得る。統合ポリシーサーバ 22 は、さらに、QoS テーブル 120 を利用し、デバイス情報に基づいて適切な QoS を識別する。QoS 要求を送信するのに使用するプロトコルは、好ましくは、LDAP または COPS である。

【0040】一般に、データ通信スイッチ 18 からユーザ情報およびデバイス情報を受信すると、統合ポリシーマネージャ 104 は、データ通信スイッチと統合ポリシーサーバ 22 の間の、好ましくは、単一の制御フローで、認証情報および QoS 情報を入手することにとりかかる。これに関し、統合ポリシーサーバは、好ましくは、受信したユーザ識別情報およびユーザ署名情報を認証テーブル 110 内に記憶されている情報と比較する。そのユーザが確認された場合、統合ポリシーサーバ 22 は、そのユーザ識別情報に関連して何らかの時間制限が適用可能かどうかを判定する。

【0041】統合ポリシーサーバ 22 は、さらに、受信したデバイス情報に基づいて適用可能な QoS を識別することにとりかかる。これに関して、統合ポリシーサーバ 22 は、フロー条件を識別して対応する QoS 処理を戻すように QoS テーブル 120 を照会する。

【0042】次に、統合ポリシーサーバ 22 は、ユーザ認証情報および QoS 情報をデータ通信スイッチ 18 に送信する。統合ポリシーサーバ 22 は、そのユーザがネットワークリソースの許可されたユーザであること、およびそのログイン試行時にネットワークリソースを使用するのをユーザが許可されていることを確認した場合、ACK 指標および/またはユーザがそれに対して許可されているネットワークリソースのリストをデータ通信スイッチ 18 に送信する。また、統合ポリシーサーバ 22

は、リソースのリストとともに、その使用に適用可能ななんらかの時間制限も送信することができる。また、統合ポリシーサーバ22は、データ通信スイッチ18に、優先順位レベル、最大帯域幅等を含む識別されたQoS処理も送信する。

【0043】認証パケットおよびQoS処理パケットは、管理インターフェース98によってデータベース100から取り込まれ、統合ポリシーマネージャ104に転送される。次に、統合ポリシーマネージャ104は、ポートドライバ106を起動し、ネットワークと通信するのにユーザによって使用されるネットワークインターフェース94上でネットワーク接続性規則を確立する。具体的には、ポートドライバは、許可されたネットワークリソースを未認証状態から認証済み状態に移転させることにより、そのリソースを使用可能にする。

【0044】また、統合ポリシーマネージャは、QoSドライバ108を起動して、スイッチ上でQoS処理を実施する。本発明の一実施形態によれば、データ通信スイッチ18は、2000年9月13日出願の「ON-SWITCH POLICYRULE CACHING FOR DATA COMMUNICATIONSWITCH」という名称の出願で開示されるように、フロー条件および受信したQoS処理を将来の使用のためにキャッシュ内に記憶することができる。この出願の内容は、参照により、本明細書に組み込まれる。

【0045】図9は、単一の統合ポリシーサーバ22を介してスイッチ18によってサポートされる統合ポリシー実施サービスの例としての流れ図である。ステップ130で、管理インターフェース98が、ユーザ情報とデバイス情報の要求をデバイス24に送信する。ステップ132で、管理インターフェース98は、要求したユーザ情報およびデバイス情報をデバイス24から受信する。ステップ134で、統合ポリシーマネージャ104は、ユーザ認証およびQoS提供を求めて、統合ポリシーサーバ22にそのユーザ情報およびデバイス情報を送信する。ステップ136で、統合ポリシーマネージャ104は、そのユーザが認証されていた場合、ユーザ認証情報およびQoS情報を受信する。ステップ138で、ユーザ認証が成功したかどうかに関する照会が行われる。認証が成功であった場合、統合ポリシーマネージャ104は、ポートドライバ106およびQoSドライバ108を起動して、適切なネットワークインターフェースを使用可能にし、また識別されたQoSをデータ通信スイッチ18上で実施する。

【0046】本発明の一実施形態によれば、スイッチ10、18は、独立モード（2つのポリシーサーバ）および統合モード（1つのポリシーサーバ）で動作するように構成することができる。選択されるモードのタイプは、好ましくは、現行のサービス構成に基づいて自動的

に決定される。

【0047】本発明は、ある特定の実施形態で説明してきたが、当分野の技術者は、変形形態を困難なく考案することができる。そのような変形形態は、いかなる意味でも、本発明の趣旨および範囲を逸脱するものではない。したがって、本発明は、具体的に説明したのとは別の仕方でも実施できることを理解されたい。このため、本発明の本実施形態は、すべての点で例示的かつ非限定的であり、本発明の範囲は、前述の説明によってではなく、頭記の特許請求の範囲およびそれと等価のものによって示されるべきものと理解されたい。

#### 【図面の簡単な説明】

【図1】統合ポリシー実施サービスをサポートする通信ネットワークを示す概略図である。

【図2】2つのポリシーサーバを介して統合ポリシー実施サービスをサポートするデータ通信スイッチを示すより詳細な概略図である。

【図3】図2のポリシーサーバの一方のサーバ内に記憶されたユーザ認証テーブルを示す例としての概略レイアウト図である。

【図4】図2のポリシーサーバの他方のサーバ内に記憶されたQoSテーブルを示す例としての概略レイアウト図である。

【図5】図2の2つのポリシーサーバを介する統合ポリシー実施サービスを示す例としての流れ図である。

【図6】単一の統合ポリシーサーバを介して統合ポリシー実施サービスをサポートするデータ通信スイッチを示すより詳細な概略図である。

【図7】図6の統合ポリシーサーバ内に記憶されたユーザ認証テーブルを示す例としての概略レイアウト図である。

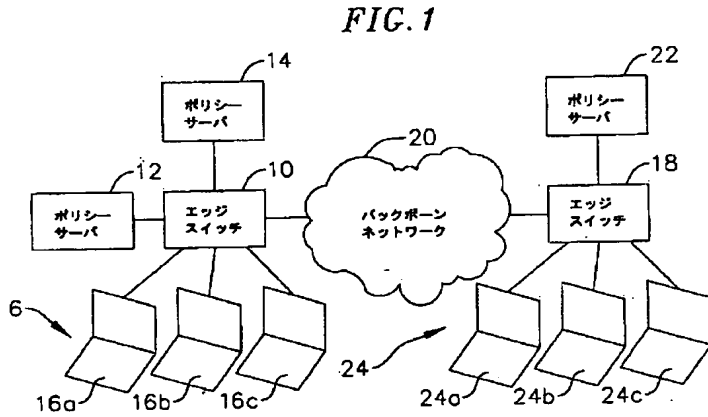
【図8】図6の統合ポリシーサーバ内に記憶されたQoSテーブルを示す例としての概略レイアウト図である。

【図9】図6の統合ポリシーサーバを介した統合ポリシー実施サービスを示す例としての流れ図である。

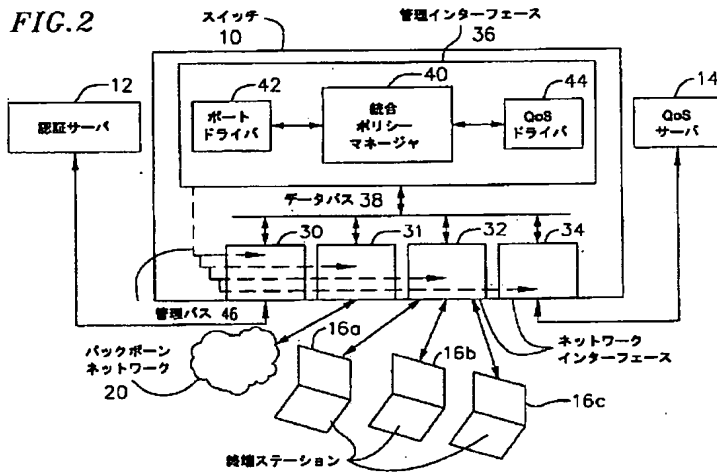
#### 【符号の説明】

- 10、18 データ通信スイッチ
- 12、14、22 ポリシーサーバ
- 16、16a、16b、16c、24、24a、24b、24c デバイス
- 20 バックボーンネットワーク
- 30、31、32、34、90、92、94、96 ネットワークインターフェース
- 36、98 管理インターフェース
- 38、100 データベース
- 40、104 統合ポリシーマネージャ
- 42、106 ポートドライバ
- 44、108 QoSドライバ
- 46、102 管理バス

【図1】



【図2】



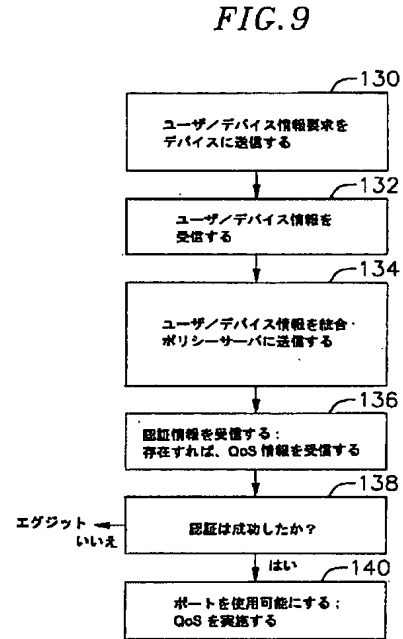
【図3】

FIG. 3

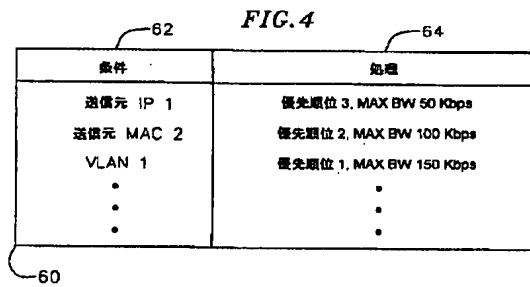
ユーザID	パスワード	許可時間	許可
ユーザ1	ユーザ1パスワード	M-F: 8AM-5PM, 12時間	ポート1, ポート2, ポート8
ユーザ2	ユーザ2パスワード	M, W, F: 5PM-8PM, 10時間	ポート3
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

50

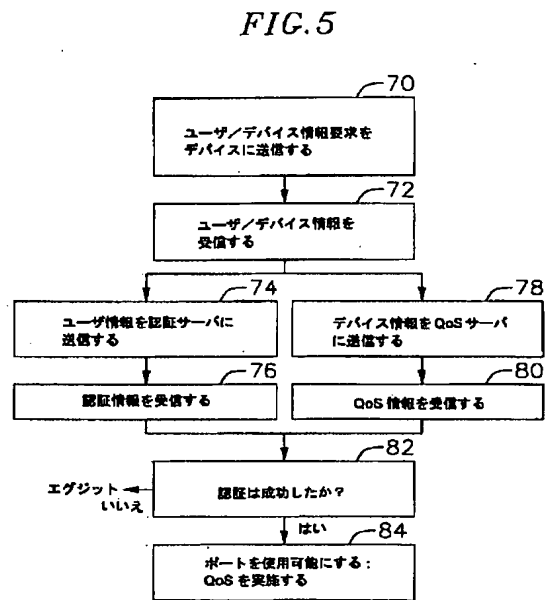
【図9】



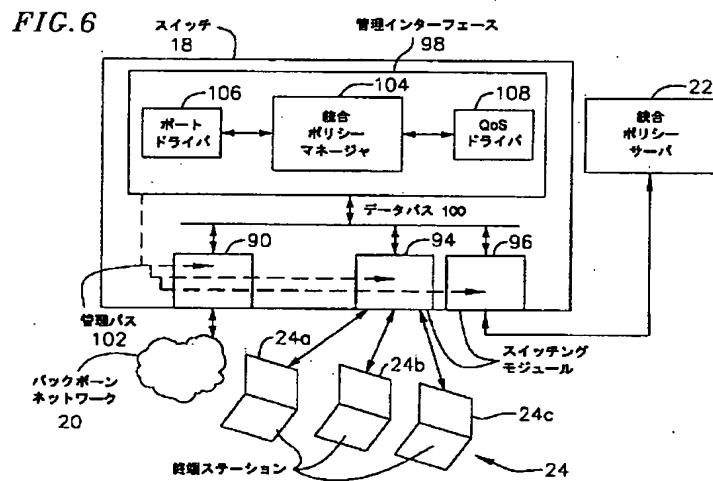
【図4】



【図5】



【図6】



【図 7】

**FIG. 7**

112 ユーザ ID	114 パスワード	116 許可時間	118 許可
ユーザ 1	ユーザ 1 パスワード	M-F, 8AM-6PM, 12 時間	ポート 1, ポート 2, ポート 6
ユーザ 2	ユーザ 2 パスワード	M, W, F, 5PM-6PM, 10 時間	ポート 3
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

110

【図 8】

**FIG. 8**

122 条件	124 処理
送信元 IP 1	優先順位 3, MAX BW 50 Kbps
送信元 MAC 2	優先順位 2, MAX BW 100 Kbps
VLAN 1	優先順位 1, MAX BW 150 Kbps
⋮	⋮
⋮	⋮

120

フロントページの続き

(72)発明者 クリストファー・マーティン  
アメリカ合衆国、ノース・カロライナ・  
27502、アベックス、ベクトン・コート・  
4404

F ターム(参考) 5B085 AE02 AE23 BG07 CA04  
5K030 GA15 HA08 HC01 HD06 JT03  
KA01 KA07 KA13 LD19  
5K033 AA08 BA08 CC01 DA01 DB14  
DB20 EA07

## 1. Title of Invention

INTEGRATED POLICY IMPLEMENTATION SERVICE  
FOR COMMUNICATION NETWORK

## 2. Claims

1. A data communication switch in a communication network including an end device and one or more policy servers, the data communication switch for use in an integrated policy implementation service for the network, the data communication switch comprising:

means for transmitting to the end device a request for a plurality of information;

means for receiving from the end device the requested plurality of information;

means for concurrently transmitting to the one or more policy servers the received plurality of information; and

means for concurrently receiving from the one or more policy servers user authentication and quality of service information, the user authentication and quality of service information being based on the transmitted plurality of information.

2. The data communication switch of claim 1, wherein the plurality of information includes user and device information.

3. The data communication switch of claim 1, wherein the switch is in communication with one policy server, the one policy server including:

means for retrieving the user authentication information;  
and

means for retrieving the quality of service information.

4. The data communication switch of claim 1, wherein the switch is in communication with two policy servers, the first policy server including means for retrieving the user authentication information and the second policy server

including means for retrieving the quality of service information.

5. The data communication switch of claim 1 further comprising means for transitioning a network resource from an unauthenticated to an authenticated state in response to the user authentication information.

6. The data communication switch of claim 1 further comprising means for implementing a quality of service on the switch in response to the quality of service information for data flows received from the end device.

7. The data communication switch of claim 1, wherein the user authentication information includes a list of authorized network resources.

8. The data communication switch of claim 1, wherein the quality of service information includes a quality of service action to be applied to data flows received from the end device.

9. The data communication switch of claim 1 further comprising:

- a first mode for supporting a single policy server;
- a second mode for supporting two policy servers; and
- means for selecting between the first mode and the second

mode.

10. A data communication switch in a communication network including an end device and a policy server, the data communication switch for use in an integrated policy implementation service for the network, the data communication switch comprising:



a first network interface transmitting to the end device a request for a plurality of information and receiving from the end device the requested plurality of information;

a management interface coupled to the first network interface, the management interface transmitting the received plurality of information to the policy server and the policy server retrieving user authentication and quality of service information in response to the plurality of information and concurrently communicating the retrieved user authentication and quality of service information to the management interface;

a first driver coupled to the management interface, the first driver transitioning a network resource from an unauthenticated to an authenticated state in response to the user authentication information; and

a second driver coupled to the management interface, the second driver implementing a quality of service on the switch for data flows received from the end device in response to the quality of service information.

11. The data communication switch of claim 10, wherein the plurality of information includes user and device information.

12. The data communication switch of claim 10, wherein the user authentication information includes a list of authorized network resources.

13. The data communication switch of claim 10, wherein the quality of service information includes a quality of service action to be applied to data flows received from end device.

14. A data communication switch in a communication network including an end device and a policy server, the data communication switch for use in an integrated policy

implementation service for the network, the data communication switch comprising:

- a first network interface transmitting to the end device a request for a plurality of information and receiving from the end device the requested plurality of information;

- a management interface coupled to the first network interface, the management interface transmitting the received plurality of information to the policy server in a single control flow and receiving user authentication and quality of service information from the policy server in the control flow;

- a first driver coupled to the management interface, the first driver transitioning a network resource from an unauthenticated to an authenticated state in response to the user authentication information; and

- a second driver coupled to the management interface, the second driver implementing a quality of service on the switch for data flows received from the end device in response to the quality of service information.

15. The data communication switch of claim 14, wherein the plurality of information includes user and device information.

16. The data communication switch of claim 14, wherein the user authentication information includes a list of authorized network resources.

17. The data communication switch of claim 14, wherein the quality of service information includes a quality of service action to be applied to data flows received from the end device.

18. A data communication switch in a communication network including an end device, a first policy server, and a second policy server, the data communication switch for use in an

integrated policy implementation service for the network, the data communication switch comprising:

- a first network interface transmitting to the end device a request for a plurality of information and receiving from the end device the requested plurality of information;

- a management interface coupled to the first network interface transmitting to the first policy server in a first control flow a first portion of the plurality of the information and receiving from the first policy server in the first control flow user authentication information, the management interface further transmitting to the second policy server in a second control flow a second portion of the plurality of the information and receiving from the second policy server in the second control flow a quality of service information, wherein the first control flow occurs concurrently with the second control flow;

- a first driver coupled to the management interface, the first driver transitioning a network resource from an unauthenticated to an authenticated state in response to the user authentication information; and

- a second driver coupled to the management interface, the second driver implementing a quality of service on the switch for data flows received from the end device in response to the quality of service information.

19. The data communication switch of claim 18, wherein the plurality of information includes user and device information.

20. The data communication switch of claim 18, wherein the user authentication information includes a list of authorized network resources.

21. The data communication switch of claim 18, wherein the quality of service information includes a quality of service action to be applied to data flows received on the switch.

22. In a communication network including an end device and one or more policy servers, a method for integrated policy implementation service for the network comprising:

transmitting to the end device a request for a plurality of information;

receiving from the end device the requested plurality of information;

transmitting to the one or more policy servers the received plurality of information; and

receiving from the one or more policy servers user authentication information concurrently with quality of service information, the user authentication and quality of service information being based on the transmitted plurality of information.

23. The method of claim 22, wherein the plurality of information includes user and device information.

24. The method of claim 22 further comprising:

retrieving the user authentication information; and

retrieving the quality of service information.

25. The method of claim 22 further comprising transitioning a network resource from an unauthenticated to an authenticated state in response to the user authentication information.

26. The method of claim 22 further comprising implementing a quality of service on the switch for data flows received from

the end device in response to the quality of service information.

27. The method of claim 22, wherein the user authentication information includes a list of authorized network resources.

28. The method of claim 22, wherein the quality of service information includes a quality of service action to be applied to data flows received on the switch.

29. The method of claim 22 further comprising selecting between a first mode supporting a single policy server and a second mode supporting two policy servers.

30. In a communication network including a switch communicating with an end device, a first policy server, and a second policy server, a method for integrated policy implementation service for the network comprising:

- transmitting to the end device a request for a plurality of information;

- receiving from the end device the requested plurality of information;

- transmitting to the first policy server in a first control flow a first portion of the plurality of the information and receiving from the first policy server in the first control flow user authentication information; and

- transmitting to the second policy server in a second control flow a second portion of the plurality of the information and receiving from the second policy server in the second control flow a quality of service information;

- wherein the first control flow occurs concurrently with the second control flow.

31. The method of claim 30, wherein the plurality of information includes user and device information.

32. The method of claim 30 further comprising transitioning a network resource from an unauthenticated to an authenticated state in response to the user authentication information.

33. The method of claim 30 further comprising implementing a quality of service on the switch for data flows received from the end device in response to the quality of service information.

34. The method of claim 30, wherein the user authentication information includes a list of authorized network resources.

35. The method of claim 30, wherein the quality of service information includes a quality of service action to be applied to data flows received on the switch.

### **3. Detailed Description of Invention**

#### **FIELD OF THE INVENTION**

The present invention relates generally to data communication networks, and more particularly, data communication networks integrating user authentication and quality of service provisioning into a single policy service.

#### **BACKGROUND OF THE INVENTION**

Data communication networks are becoming more and more intelligent. One service increasing the intelligence of networks is user authentication. User authentication answers the question of whether a user may communicate in the network. Whereas legacy networks provided users unrestricted access the network, more recent vintage networks permit a user to communicate only after verifying the user's identity, and even then may allow the user to communicate only with a subset of network devices.

Another service raising the intelligence of networks is quality of service (QoS) provisioning. QoS provisioning addresses the question of how well a user may communicate in the network. Whereas legacy networks provided first-in-time delivery of packets, more recent vintage networks depart from first-in-time packet ordering and provide different QoS for different data flows.

QoS applies policy rules to the flows seen on the network. A policy rule generally includes a flow condition component and a QoS action component, and answers the question of what action should be applied to a flow meeting a particular condition. For example, a simple policy rule may take the form "treat traffic

in group 2 at priority level 3," in which case the flow condition is "group 2" and the QoS action is "priority level 3."

While user authentication and QoS provisioning services have created more intelligent networks, they have not been tightly integrated. Typically, the QoS provisioning task has only been initiated after the user authentication task has been successfully completed. Duplication of effort and unnecessary delay have therefore resulted from such serialized policy provisioning.

#### SUMMARY OF THE INVENTION

The present invention comprises an integrated policy implementation service for a communication network where user authentication is integrated with QoS provisioning.

In one aspect of the invention, a data communication switch supports the integrated policy implementation service via a single integrated policy server. The switch includes a first network interface that transmits to an end device a request for user and device information, and receives from the end device the requested user and device information. The user information may include a user identifier and password. The device information may include Layer 2 and/or Layer 3 information such as, for example, MAC addresses, Internet Protocol (IP) addresses, and virtual LAN (VLAN) identifiers.

The data communication switch includes a management interface that transmits the received user and device information to the policy server and receives user authentication and quality of service information in a single control flow between the management interface and the policy server. The authentication information may include ACK/NACK indicators and/or lists of authorized ports or devices. The QoS



information may include priority and maximum bandwidth information.

The data communication switch also includes a first driver, such as, for example, a port driver, that transitions a network resource from an unauthenticated to an authenticated state in response to the user authentication information. In addition, a second driver, such as, for example, a QoS driver, implements a quality of service on the switch for data flows received from the data communication switch in response to the quality of service information.

In another aspect of the invention, the data communication switch supports the integrated policy implementation service via two independent policy servers. The switch includes a management interface that transmits the received user information to a first policy server in a first control flow and receives user authentication information from the first policy server in the first control flow. The management interface further transmits the received device information to a second policy server in a second control flow and receives quality of service information from the second policy server in the second control flow. The first and second control flows preferably occur in parallel. Such parallel execution of user authentication and QoS provisioning helps reduce the delays associated with serialized policy provisioning existing in the prior art.

#### DETAILED DESCRIPTION OF THE SPECIFIC EMBODIMENTS

FIG. 1 is a schematic diagram of a communication network supporting an integrated policy implementation service. The network includes a data communication switch 10 coupled to policy servers 12, 14 and devices 16a, 16b, 16c. The data communication switch 10 is coupled to data communication switch 18 across a backbone network 20 via one or more core switches (not shown) operative in the backbone network. Data communication switch 18 is also coupled to a policy server 22 and devices 24a, 24b, 24c.

The devices 16, 24 are preferably network end-stations, such as, for example, personal computers, workstations, or

servers, having respective network interfaces for packetized communication with other devices via the data communication switches 10, 18. The data communication switches 10, 18 are preferably gateway devices such as, for example, hubs, bridges, or routers, having a plurality of respective network interfaces for forwarding packetized communications originated by the devices 16, 24. The policy servers 12, 14, 22 preferably provide authentication and QoS provisioning services to the data communication switches 10, 18. The devices 16, 24, data communication switches 10, 18, and policy servers 12, 14, 22 may be interconnected via cables or other transmission media, and may support various data communication protocols, such as, for example, Ethernet, Internet Protocol, and Asynchronous Transfer Mode (ATM).

Integrated policy implementation service is discussed in general terms with respect to the data communication switch 10 and policy servers 12, 14. The data communication switch 10 preferably transmits requests for user and device information to the devices 16 connected to the network. The devices 16 preferably respond by transmitting responses including the user and device information to the switch 10. The switch 10 preferably transmits the received user and device information to the policy servers 12, 14 for user authentication and QoS provisioning. The policy servers 12, 14 preferably respond by transmitting authentication information and QoS information to the switch 10. The switch 10 preferably uses the authentication information to determine whether to enable a network interface used by the user to communicate with the network. To the extent a determination is made to enable the network interface, the switch preferably uses the received QoS information to establish a QoS on the switch. The QoS is then applied to the traffic

received from the device used by the user to communicate with the network.

According to one embodiment of the invention, the integrated policy implementation service configuration preferably includes two independent policy servers as is illustrated by data communication switch 10 and policy servers 12, 14. FIG. 2 is a more detailed schematic diagram of the data communication switch 10 supporting an integrated policy implementation service via the two policy servers 12, 14 (also referred to as authentication and QoS servers). The data communication switch 10 includes network interfaces 30, 31, 32, 34 and a management interface 36 linked by a data bus 38. The network interfaces 30, 31, 32, 34 interconnect the devices 16, switches in the backbone network 20, and policy servers 12, 14 over different interfaces.

The management interface 36 and network interfaces 30, 31, 32, 34 are coupled to the data bus 38 for transmitting and receiving data traffic. The management interface 36 and network interfaces 30, 31, 32, 34 are also coupled to a management bus 46 for transmitting and receiving management information preferably including authentication and QoS information.

The management interface 36 supports various modules, including an integrated policy manager 40, port driver 42, and QoS driver 44. The integrated policy manager 40, port driver 42, and QoS driver 44 are preferably software modules. Alternatively, implementation of the system may be accomplished in a combination of hardware, firmware (e.g. application specific integrated circuits or other customized circuits), and/or software, or by any method known in the art.

According to one embodiment of the invention, the data communication switch 10 supports integrated policy implementation in the following manner. The integrated policy

manager 40 transmits user and device information requests via the management bus 46 to the devices 16.

The devices 16 respond by transmitting the user and device information via the data bus 38. The user information preferably includes user identification information, such as, for example, a user ID, and user signature information, such as, for example, a password. The device information preferably includes Layer 2 and/or Layer 3 information, such as, for example, MAC addresses, IP addresses, VLAN identifiers, and the like. It should be understood, however, that one or more of such device information (e.g. the MAC address) may already be known to the data communication switch 10 via source learning. In this scenario, the known device address may not need to be expressly transmitted to the data communication switch.

The user and device information packets are captured off the data bus 38 by the management interface 36 and forwarded to the integrated policy manager 40. The integrated policy manager 40 proceeds to determine whether a particular user is authorized to communicate in the network and identify the QoS designed for the user device. In this regard, the integrated policy manager 40, in a first control flow, transmits the received user information to one of the policy servers, namely, the authentication server 12, and receives a corresponding authentication information from the authentication server. The authentication information preferably includes ACK/NACK indicators, list of authorized ports, and/or other authenticating information. Although FIG. 2 illustrates a single authentication server, a network operating in accordance with the present invention may include one or more authentication servers.

In a second control flow, the integrated policy manager 40 transmits the received device information to the second policy

server, namely, the QoS server 14, and receives the QoS information for the device from the QoS server. The QoS information preferably includes priority levels, maximum bandwidth information, and the like.

The first and second control flows preferably occur in parallel. Such parallel execution of user authentication and QoS provisioning helps reduce the delays associated with serialized policy provisioning.

FIG. 3 is an exemplary schematic layout diagram of a user authentication table 50 stored in the authentication server 12. The authentication table 50 may be created and organized using tools such as, for example, NetWare®, which is commercially available from Novell, Inc. In one exemplary embodiment, the authentication table 50 suitably comprises a set of user authenticating information that may be arranged in a variety of ways, but is most advantageously configured as sequential entries, with each entry specific to a particular user to be authorized. A particular entry of the table 50 may include a unique user identifier 52, such as, for example, an identification number, character, or combination of numbers and characters. A particular entry may further include a user signature, such as, for example, a user password 54, for verifying the user seeking access to the network. In addition to the above, a particular entry may include time restriction information 56 as well as authorized resource information 58 for the particular user. The time restriction information preferably defines times during which the particular user is authorized to use the network resources, such as, for example, the day of the week, time of the day, and length of permitted access. The list of authorized network resources is preferably a list of authorized network interfaces and/or devices.

The authentication server 12 preferably utilizes the authentication table 50 to authorize a user in the manner described in U.S. Patent No. 6,070,243, the contents of which are hereby incorporated by reference. The protocol used for user authentication may include RADIUS, LDAP (Lightweight Directory Access Protocol), COPS (Common Open Policy Service), or any other authentication protocol known in the art, either alone or in combination.

In general terms, however, upon receipt of the user information from the data communication switch 10, the authentication server 12 preferably compares the received information with the user identification and signature information stored in the server 12. The authentication server 12 may further determine whether any time restrictions associated with the user identification information are applicable. If the authentication server 12 verifies that the user is an authorized user of the network resources, and that the user is authorized to use the network resources at the time of the log-in attempt, the server preferably transmits to the data communication switch 10 an ACK indicator and/or the list of network resources for which the user is authorized. The authentication server 12 may also transmit, along with the list of resources, any time restrictions applicable to the usage. The integrated policy manager 40 may then invoke the port driver 42 to establish network connectivity rules on the network interface 32 used by the user to communicate with the network. Specifically, the port driver preferably enables the authorized network resources by transitioning them from an unauthenticated state to an authenticated state. The integrated policy manager 40 may also perform time restriction processing based on the time restriction information 56.

FIG. 4 is an exemplary schematic layout diagram of a QoS table 60 stored in the QoS server 14. The QoS table 60 preferably comprises a set of flow conditions 62 and QoS actions 64 matching each of the flow conditions. The flow conditions 62 may include MAC addresses, IP addresses, VLAN identifiers, slot/port identifiers, IP protocols, interface types, and the like. The QoS actions 64 specify at least a priority level indicative of a priority given to traffic meeting the flow condition. The QoS actions 64 may further indicate a maximum bandwidth, minimum bandwidth, peak bandwidth, priority, latency, jitter, maximum queue depth, maximum queue buffers, and the like.

In identifying an applicable QoS for the traffic received from the device, the integrated policy manager 40 preferably uses LDAP or COPS to transmit a QoS request with the device information to the QoS server 14. Upon receipt of the device information, the QoS server 14 identifies a flow condition and returns the corresponding QoS action to the data communication switch 10. The QoS action packets are captured off the data bus 38 by the management interface 36 and forwarded to the integrated policy manager 40. The integrated policy manager 40 then notifies the QoS driver 44 to implement the QoS action on the switch. According to one embodiment of the invention, the data communication switch 10 may store the flow condition and the received QoS action in a cache for future use, as is disclosed in the application entitled "ON-SWITCH POLICY RULE CACHING FOR DATA COMMUNICATION SWITCH," filed on September 13, 2000, the contents of which are hereby incorporated by reference.

FIG. 5 is an exemplary flow diagram of an integrated policy implementation service supported by the switch 10 via the two policy servers 12, 14. In step 70, the management interface

36 preferably transmits a user and device information request to the devices 16. In step 72, the management interface 36 receives the requested user and device information from the devices 16. In a first control flow indicated by steps 74 and 76, the integrated policy manager 40 transmits a user authentication request with the user information to the authentication server 12 and receives back the user authentication information indicating whether the user has been authenticated.

In a second control flow indicated by steps 78 and 80, the integrated policy manager 40 transmits a QoS request with the device information to QoS server 14 and receives back the QoS information for the traffic originating from the device. The first and second control flows preferably over in parallel.

In step 82, an inquiry is made as to whether the user authentication was successful. If the authentication was successful, the integrated policy manager 40 preferably invokes the port driver 42 and the QoS driver 44 to enable the appropriate network interface and implement the identified QoS on the data communication switch 10.

According to an alternative embodiment of the invention, the integrated policy implementation service configuration includes a single integrated policy server, as is illustrated by data communication switch 18 and policy server 22. FIG. 6 is a more detailed schematic diagram of the data communication switch 18 supporting an integrated policy implementation service via the single policy server 22 (also referred to as an integrated policy server). The data communication switch 18 includes network interfaces 90, 92, 94, 96 and management interface 98 linked by data bus 100. The network interfaces 90, 92, 94, 96 interconnect the devices 24, switches in the backbone



network 20, and integrated policy server 22 over different interfaces.

The management interface 98 and network interfaces 90, 92, 94, 96 are coupled to the data bus 100 for transmitting and receiving data traffic. The management interface 98 and network interfaces 90, 92, 94, 96 are also coupled to a management bus 102 for transmitting and receiving management information including authentication and QoS information.

The management interface 98 supports various modules, including an integrated policy manager 104, port driver 106, and QoS driver 108. The policy manager 104, port driver 106, and QoS driver 108 are preferably software modules. Alternatively, implementation of the system may be accomplished in a combination of hardware, firmware (e.g. application specific integrated circuits or other customized circuits), and/or software, or by any method known in the art.

According to one embodiment of the invention, the data communication switch 18 supports integrated policy implementation in the following manner. The integrated policy preferably manager 104 transmits user and device information requests via the management bus 102 to the devices 24.

The devices 24 respond by transmitting the user and device information via the data bus 100. The user information preferably includes user identification information, such as, for example, a user ID, and user signature information, such as, for example, a password. The device information preferably includes Layer 2 and/or Layer 3 information, such as, for example, MAC addresses, IP addresses, virtual LAN identifiers, and the like. It should be understood, however, that one or more of such device information (e.g. the MAC address) may already be known to the data communication switch 18 via source learning. In this scenario, the known device address may not

need to be expressly transmitted to the data communication switch.

The user and device information packets are captured off the data bus 100 by the management interface 98 and forwarded to the integrated policy manager 104. The integrated policy manager 104 proceeds to determine whether a particular user is authorized to communicate in the network and identify the QoS designed for the user device. In this regard, the integrated policy manager 104, preferably in a single control flow, transmits to the integrated policy server 22 the received user and device information, and receives from the integrated policy server 22 a corresponding authentication and QoS information. The authentication information preferably includes ACK/NACK indicators, list of authorized parts, and/or other authenticating information. The QoS information preferably includes priority levels, maximum bandwidth information, and the like.

FIG. 7 is an exemplary schematic layout diagram of a user authentication table 110 stored in the integrated policy server 22. The authentication table 50 may be created and organized using tools such as, for example, NetWare®, which is commercially available from Novell, Inc. In one exemplary embodiment, the authentication table 110 suitably comprises a set of user authenticating information that may be arranged in a variety of ways, but is most advantageously configured as sequential entries, with each entry specific to a particular user to be authorized. A particular entry of the table 110 includes a unique user identifier 112, such as, for example, an identification number, character, or combination of numbers and characters. A particular entry further includes a user signature, such as, for example, a user password 114, for verifying the user seeking access to the network. In addition

to the above, a particular entry includes time restriction information 116 as well as authorized resource information 118 for the particular user. The time restriction information preferably defines times during which the particular user is authorized to use the network resources, such as, for example, the day of the week, time of the day, and length of permitted access. The list of authorized network resources is preferably a list of authorized network interfaces and/or devices.

FIG. 8 is an exemplary schematic layout diagram of a QoS table 120 also stored in the integrated policy server 22. The QoS table 120 preferably comprises a set of flow conditions 122 and QoS actions 124 matching each of the flow conditions. The flow conditions 122 preferably include MAC addresses, IP addresses, VLAN identifiers, slot/port identifiers, IP protocols, interface types, and the like. The QoS actions 124 specify at least a priority level indicative of a priority given to traffic meeting the flow condition. The QoS actions 124 may further indicate a maximum bandwidth, minimum bandwidth, peak bandwidth, priority, latency, jitter, maximum queue depth, maximum queue buffers, and the like.

According to one embodiment of the invention, the authentication and QoS tables 110, 120 are stored in one or more databases hosted by the integrated policy server 22. The database(s) preferably reside in one or more mass storage devices, such as, for example, hard disk drives, or drive arrays.

The integrated policy server 22 preferably utilizes the authentication table 110 to authorize a user in the manner described in U.S. Patent No. 6,070,243, the contents of which are hereby incorporated by reference. The protocol used for user authentication may include RADIUS, LDAP (Lightweight Directory Access Protocol), COPS, or any other authentication

protocol known in the art, either alone or in combination. The integrated policy server 22 further uses the QoS table 120 to identify the appropriate QoS based on the device information. The protocol used to transmit a QoS request is preferably LDAP or COPS.

In general terms, upon receipt of the user and device information from the data communication switch 18, the integrated policy manager 104 proceeds to obtain the authentication and QoS information preferably in a single control flow between the data communication switch and the integrated policy server 22. In this regard, the integrated policy server preferably compares the received user identification and signature information with the information stored in the authentication table 110. If the user is verified, the integrated policy server 22 also determines whether any time restrictions associated with the user identification information are applicable.

The integrated policy server 22 further proceeds to identify an applicable QoS based on the received device information. In this regard, the integrated policy server 22 interrogates the QoS table 120 to identify a flow condition and returns the corresponding QoS action.

The integrated policy server 22 then transmits the user authentication and QoS information to the data communication switch 18. If the integrated policy server 22 verifies that the user is an authorized user of the network resources, and that the user is authorized to use the network resources at the time of the log-in attempt, the server transmits to the data communication switch 22 an ACK indicator and/or the list of network resources for which the user is authorized. The integrated policy server 22 may also transmit, along with the list of resources, any time restrictions applicable to the

usage. The integrated policy server 22 also transmits to the data communication switch 18 the identified QoS action including priority level, maximum bandwidth, and the like.

The authentication and QoS action packets are captured off the data bus 100 by the management interface 98 and forwarded to the integrated policy manager 104. The integrated policy manager 104 then invokes the port driver 106 to establish network connectivity rules on the network interface 94 used by the user to communicate with the network. Specifically, the port driver enables the authorized network resources by transitioning them from an unauthenticated state to an authenticated state.

The integrated policy manager also invokes the QoS driver 108 to implement the QoS action on the switch. According to one embodiment of the invention, the data communication switch 18 may store the flow condition and the received QoS action, in the cache for future use, as is disclosed in the application entitled "ON-SWITCH POLICY RULE CACHING FOR DATA COMMUNICATION SWITCH," filed on September 13, 2000, the contents of which are hereby incorporated by reference.

FIG. 9 is an exemplary flow diagram of an integrated policy implementation service supported by the switch 18 via the single integrated policy server 22. In step 130, the management interface 98 transmits a user and device information request to the devices 24. In step 132, the management interface 98 receives the requested user and device information from the devices 24. In step 134, the integrated policy manager 104 transmits the user and device information to the integrated policy server 22 in a request for user authentication and QoS provisioning. In step 136, the integrated policy manager 104 receives the user authentication information and QoS information if the user has been authenticated. In step 138, an inquiry is

made as to whether the user authentication was successful. If the authentication was successful, the integrated policy manager 104 invokes the port driver 106 and QoS driver 108 to enable the appropriate network interface and implement the identified QoS on the data communication switch 18.

According to one embodiment of the invention, the switches 10, 18 may be arranged to be operative in independent (two policy servers) and integrated (one policy server) modes. The type of mode selected is preferably automatically determined based on the current service configuration.

Although this invention has been described in certain specific embodiments, those skilled in the art will have no difficulty devising variations which in no way depart from the scope and spirit of the present invention. It is therefore to be understood that this invention may be practiced otherwise than is specifically described. Thus, the present embodiments of the invention should be considered in all respects as illustrative and not restrictive, the scope of the invention to be indicated by the appended claims and their equivalents rather than the foregoing description.

#### 4. Brief Description of Drawings

FIG. 1 is a schematic diagram of a communication network supporting an integrated policy implementation service.

FIG. 2 is a more detailed schematic diagram of a data communication switch supporting an integrated policy implementation service via two policy servers.

FIG. 3 is an exemplary schematic layout diagram of a user authentication table stored in one of the policy servers of FIG. 2.

FIG. 4 is an exemplary schematic layout diagram of a QoS table stored in the other policy server of FIG. 2.

FIG. 5 is an exemplary flow diagram of an integrated policy implementation service via the two policy servers of FIG. 2.

FIG. 6 is a more detailed schematic diagram of a data communication switch supporting an integrated policy implementation service via a single integrated policy server.

FIG. 7 is an exemplary schematic layout diagram of a user authentication table stored in the integrated policy server of FIG. 6.

FIG. 8 is an exemplary schematic layout diagram of a QoS table stored in the integrated policy server of FIG. 6.

FIG. 9 is an exemplary flow diagram of an integrated policy implementation service via the integrated policy server of FIG. 6.

Fig. 1

FIG. 1

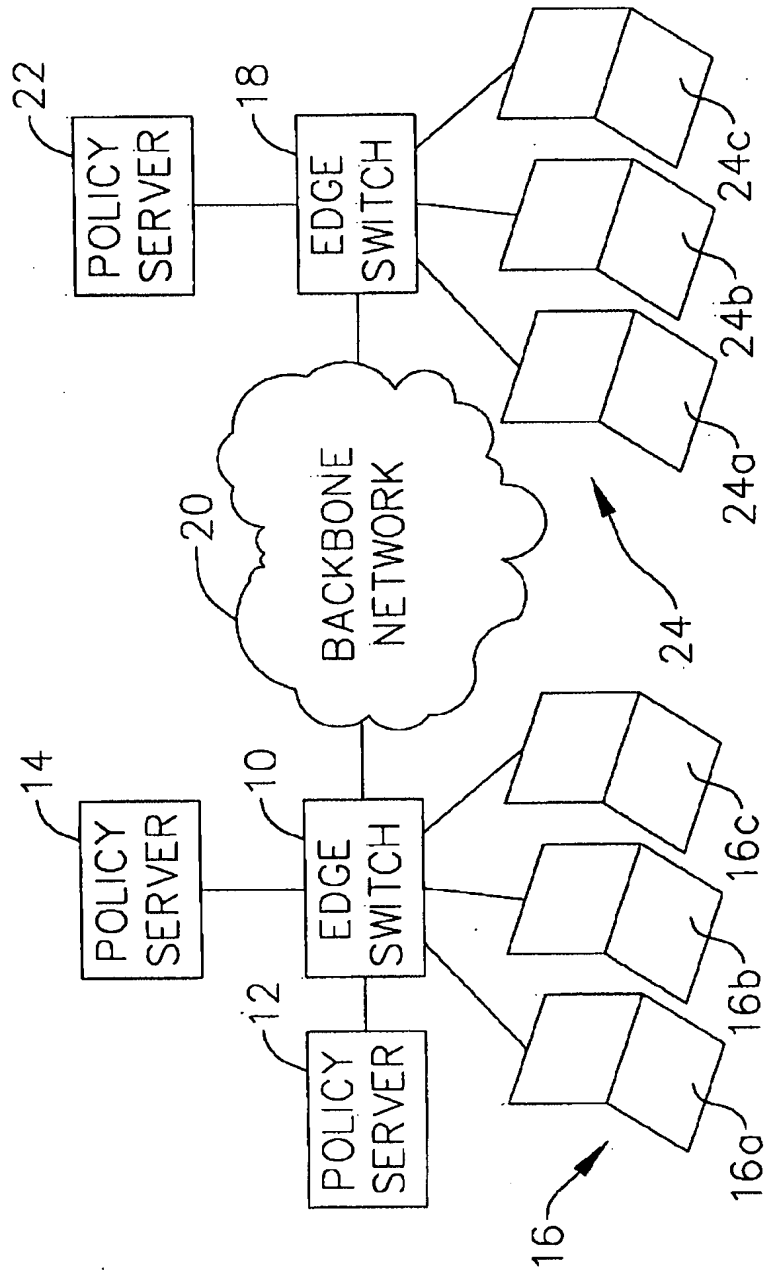




Fig. 2

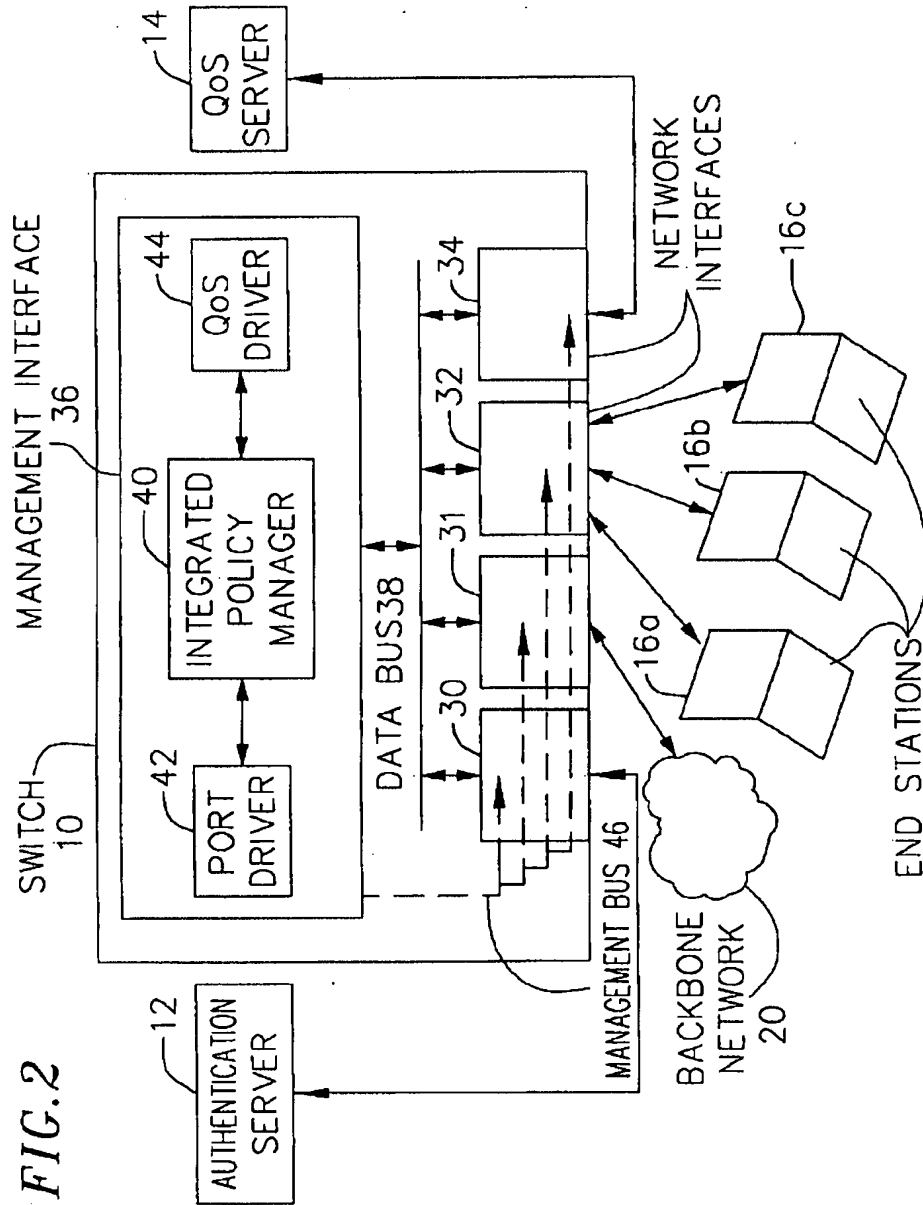


Fig. 3

**FIG. 3**

USER ID	PASSWORD	AUTHORIZED TIME	AUTHORIZED
USER 1	USER 1 PASS	M-F; 8AM-5PM; 12HOUR	PORT 1, PORT 2, PORT 6
USER 2	USER 2 PASS	M,W,F; 5PM-9PM; 10 HOURS	PORT 3
•	•	•	•
•	•	•	•
•	•	•	•

**Fig. 4**

**FIG. 4**

CONDITION	ACTION
SOURCE IP 1	PRIORITY 3, MAX BW 50 Kbps
SOURCE MAC 2	PRIORITY 2, MAX BW 100 Kbps
VLAN 1	PRIORITY 1, MAX BW 150 Kbps
• • •	• • •

Fig. 5

FIG. 5

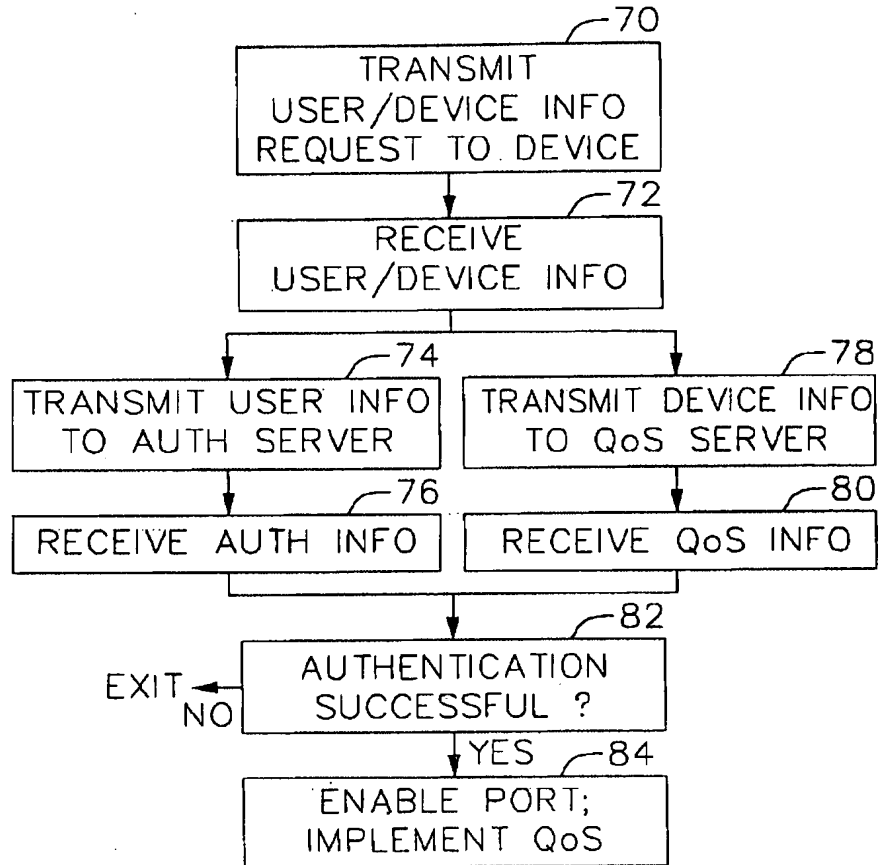


Fig. 6

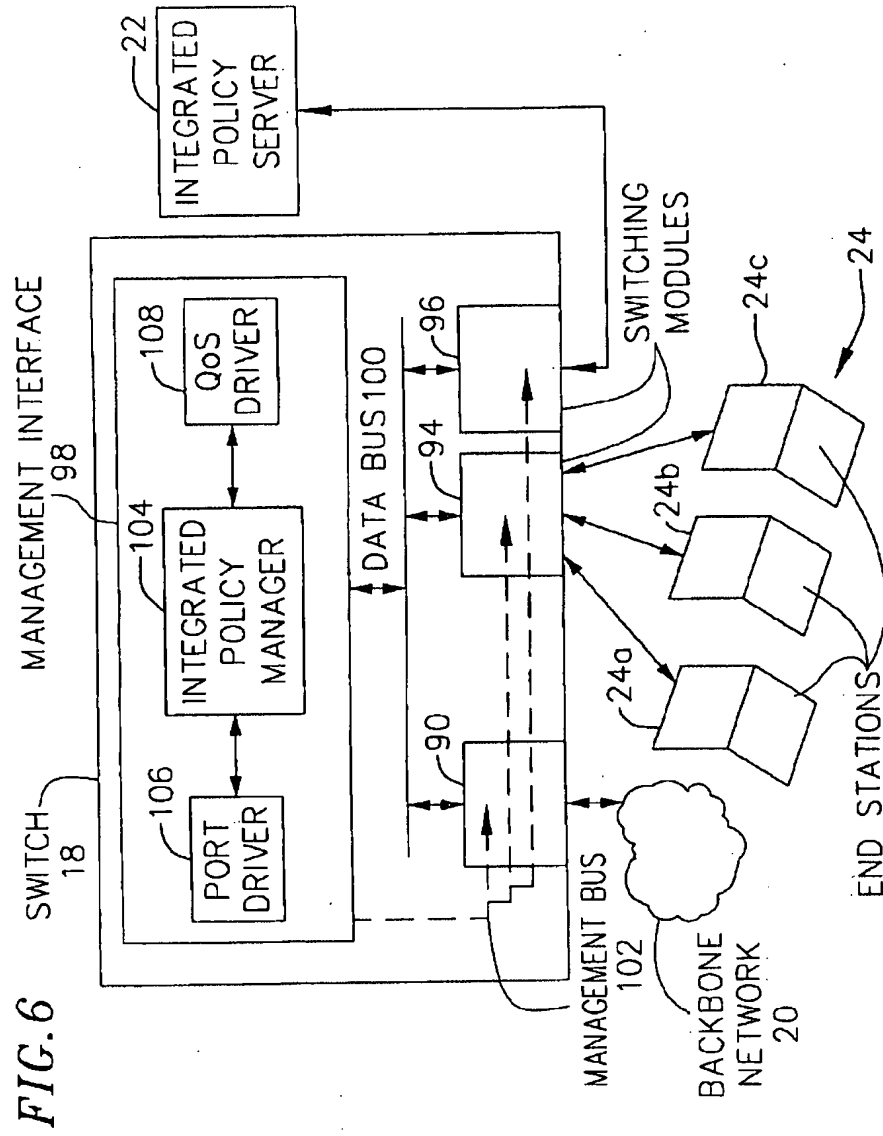


Fig. 7

**FIG. 7**

USER ID	PASSWORD	AUTHORIZED TIME	AUTHORIZED
USER 1	USER 1 PASS	M-F; 8AM-5PM; 12HOUR	PORT 1, PORT 2, PORT 6
USER 2	USER 2 PASS	M,W,F; 5PM-9PM; 10 HOURS	PORT 3
•	•	•	•
•	•	•	•
•	•	•	•

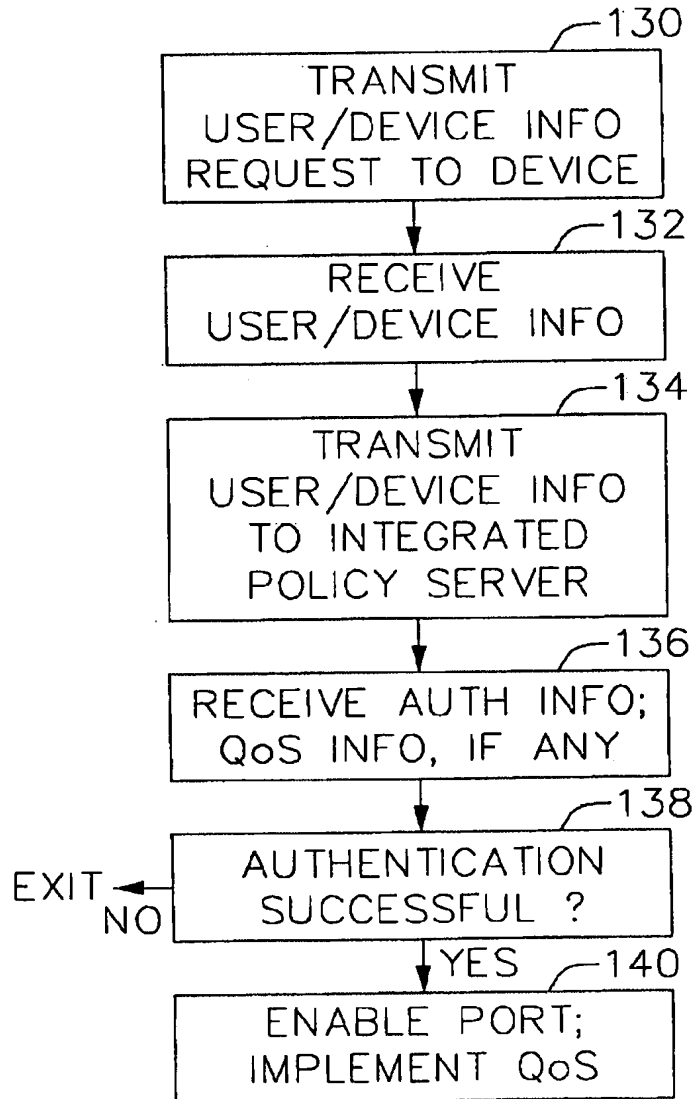
Fig. 8

FIG. 8

CONDITION	ACTION
SOURCE IP 1	PRIORITY 3, MAX BW 50 Kbps
SOURCE MAC 2	PRIORITY 2, MAX BW 100 Kbps
VLAN 1	PRIORITY 1, MAX BW 150 Kbps
•	•
•	•
•	•

Fig. 9

FIG. 9





## **1. Abstract**

An integrated policy implementation service for a communication network where user authentication is integrated with QoS provisioning. The service includes a data communication switch connected to one or more policy servers. The switch transmits requests for user and device information to the end devices connected to the network. The devices respond by transmitting responses including the user and device information to the switch. The switch transmits the user and device information to the one or more policy servers for user authentication and QoS provisioning. The one or more policy servers respond by transmitting authentication information and QoS information to the switch. The switch uses the authentication information to determine whether to enable a network interface used by the user to communicate with the network. To the extent a determination is made to enable the network interface, the switch uses the received QoS information to establish a QoS on the switch. The QoS is then applied to the traffic received from the device used by the user to communicate with the network.

## **2. Representative Drawing**

**Fig. 1**